

UNITED STATES DISTRICT COURT

for the
Southern District of Texas

JAN 28 2022

NATHAN OCHSNER
CLERK OF COURT

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)Dropbox Inc., 1800 Owens St. Ste. 200 San Francisco,
CA 94158 for accounts associated with email
danielmolstad380@gmail.com

Case No. 1:22-MJ-166

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

Dropbox Inc., 1800 Owens St. Ste. 200 San Francisco, CA 94158

See attachment "A"

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

See attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 USC 2252 and 18 USC
2252AOffense Description
knowingly possess, receive or distribute, by computer or mail, any visual depiction of minors engaging in sexually explicit conduct that has been mailed or shipped or transported in interstate or foreign commerce.

The application is based on these facts:

See attachment "C"

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Submitted by reliable electronic means, sworn to and
signature attested as per Fed. Rules Cr. Proc. 4.1

Date: January 28, 2022

City and state: Brownsville, Texas

Applicant's signature

Ian Kelly, Special Agent

Printed name and title

Judge's signature

Ignacio Torteya III, United States Magistrate Judge

Printed name and title

1:22-MJ-166

JAN 28 2022

UNITED STATES DISTRICT COURT FOR THE
SOUTHERN DISTRICT OF TEXAS

NATHAN OCHSNER
CLERK OF COURT

IN THE MATTER OF THE SEARCH OF:

Dropbox, Inc. account registered to the email address: danielmolstad380@gmail.com

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

ATTACHMENT C

I, Ian M. Kelly, being duly sworn, depose and say that:

1. I have over thirteen (13) years of federal law enforcement experience and have been employed as a Special Agent (SA) with the Department of Homeland Security (DHS) Homeland Security Investigations (HSI), since 2017, and am currently assigned to the Rio Grande Valley Child Exploitation Investigations Task Force (RGV CEITF). I have gained experience through training at the Federal Law Enforcement Training Center (FLETC) and everyday work relating to conducting these types of investigations. In addition, I have a master's degree in Management, Strategy and Leadership from Michigan State University. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2252 and 2252A, and I am authorized by law to request a search warrant.
2. As part of my official duties, I have conducted and participated in investigations relating to the sexual exploitation of children. During these investigations, I have observed and reviewed examples of child pornography in various forms of media, including computer media. I have also received training and instruction in the field of investigating child pornography.
3. This affidavit is being submitted in support of an Application for a Search Warrant for information associated with an email account that is stored at the premises owned, maintained, controlled, or operated by Dropbox, Inc. headquarter at: Dropbox, Inc., 1800 Owens St. Ste. 200 San Francisco, CA 94158. The information to be searched is described in the following paragraphs and in Attachment "A". This affidavit is made in support of an application for a search warrant under 18 USC 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Dropbox, Inc. to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the accounts, including the contents of communications.
4. The information contained in this Affidavit is based upon my personal knowledge and observation, my training and experience, conversations with other law enforcement officers and witnesses, and the review of documents and records. This affidavit is submitted in support of an application for a search warrant authorizing the search and seizure of the Dropbox, Inc. account registered to the email address: danielmolstad380@gmail.com. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not set forth every fact of this investigation.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18 United States Code, Section 2252 and 2252A have been committed by the registered owner of email danielmolstad380@gmail.com. There is probable cause to search the information described in Attachment "A" for evidence of these crimes and contraband or fruits of these crimes as described in Attachment "B".

APPLICABLE LAW

6. This investigation concerns alleged violations of Title 18, United States Code, Sections 2252 and 2252A, relating to material involving the sexual exploitation of minors.

6.1 18 U.S.C. § 2252(a) (1) prohibits a person from knowingly transporting or shipping in interstate or foreign commerce, by computer or mail, any visual depiction of minors engaging in sexually explicit conduct. Under 18 U.S.C. § 2252(a) (2), it is a federal crime for any person to knowingly receive or distribute, by computer or mail, any visual depiction of minors engaging in sexually explicit conduct that has been mailed or shipped or transported in interstate or foreign commerce. That section also makes it a federal crime for any person to knowingly reproduce any visual depiction of minors engaging in sexually explicit conduct for distribution in interstate or foreign commerce by any means, including by computer or the mail. Under 18 U.S.C. § 2252 (a) (4), it is also a crime for a person to possess one or more books, magazines, periodicals, films, or other materials which contain visual depictions of minors engaged in sexually explicit conduct that have been transported in interstate or foreign commerce or that were produced using materials that had traveled in interstate or foreign commerce.

6.2 18 U.S.C. § 2252A (a) (1) prohibits a person from knowingly mailing, transporting, or shipping child pornography in interstate or foreign commerce by any means, including by computer. 18 U.S.C. § 2252A(a) (2) prohibits a person from knowingly receiving or distributing any child pornography that has been mailed or shipped or transported in interstate or foreign commerce by any means, including by computer. 18 U.S.C. § 2252A (a) (3) prohibits a person from knowingly reproducing child pornography for distribution through the mail or in interstate or foreign commerce by any means, including by computer. 18 U.S.C. § 2252A (a) (5) (B) prohibits a person from knowingly possessing any book, magazine, periodical, film, videotape, computer disk, or other material that contains an image of child pornography that has been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer.

7. Per 18 USC Section 2256 (1), the term "minor" means any person under the age of eighteen years.

8. Per 18 USC Section 2256 (8), the term "child pornography" means any visual depiction, including any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where:

- (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;
- (B) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or
- (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

9. Per 18 U.S.C. Section 2256(2) (A), except as provided in subparagraph B, "sexually explicit conduct" means actual or simulated –

- (i) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex;
- (ii) bestiality;
- (iii) masturbation;
- (iv) sadistic or masochistic abuse; or
- (v) lascivious exhibition of the genitals or pubic area of any person;

(B) For purposes of subsection 8 (B) of this section, "sexually explicit conduct" means

- (i) graphic sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex, or lascivious simulated sexual intercourse where the genitals, breast, or pubic area of any person is exhibited;
- (ii) graphic or lascivious simulated:
 - (I) bestiality;
 - (II) masturbation; or
 - (III) sadistic or masochistic abuse; or
- (iii) graphic or simulated lascivious exhibition of the genitals or pubic area of any person.

CHILD PORNOGRAPHY ON THE INTERNET

10. Pursuant to your Affiant's training and experience, as well as the training and experience of other law enforcement personnel, your Affiant has learned that child pornography is not readily available in retail establishments. Accordingly, individuals who wish to obtain child pornography do so by ordering it from abroad or by discreet contacts with other individuals who have it available. The use of the internet to traffic in, trade, or collect child pornography has become one of the preferred methods of obtaining this material. An individual familiar with the internet can use it, usually in the privacy of his own home, to interact with another individual or a business offering such materials. The use of the internet offers individuals interested in obtaining child pornography a sense of privacy and secrecy not available elsewhere.

11. Based upon your Affiant's training and experience, your Affiant knows the following:

11.1 The internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. In order to access the internet, an individual computer user must subscribe to an access provider, which operates a host computer system with direct access to the internet. The World Wide Web (www) is a functionality of the internet, which allows users of the internet to share information;

11.2 With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. This connection can be made by any number of means, including modem, local area network, wireless and numerous other methods.

COMPUTER TERMS

12. For the purposes of this affidavit, unless otherwise specifically indicated, the term computer, as defined in 18 USC §1030(e) (1), refers to the box that houses the central processing unit (CPU), along with any internal storage devices (such as internal hard drives) and internal communication devices (such as internal modems capable of sending/receiving electronic mail or fax cards) along with any other hardware stored or housed internally. Printers, external modems (attached by cable to the main unit), monitors and other external attachments will be referred to collectively as peripherals and discussed individually when appropriate. When the computer and all peripherals are referred to as one package, the term computer system is used. Information refers to all the information on a computer system including both software applications and data.

13. The term computer hardware as used in this affidavit refers to all equipment that can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data. Hardware includes, but is not limited to, any data processing devices (such as central processing units, memory typewriters, and self-contained laptops or notebook computers); internal and peripheral storage devices, transistor-like binary devices, and other memory storage devices; peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors and optical readers); and related communications devices (such as modems, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices and electronic tone generating devices); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (such as physical keys and locks).

14. The term computer software as used in this affidavit refers to digital information, which can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, optical, or other digital form. It commonly includes programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters and communications programs.

15. The term computer-related documentation used in this affidavit refers to written, recorded, printed or electronically stored material, which explains or illustrates how to configure or use computer hardware, software or other related items.

16. Computer passwords and other data security devices are designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric, or other special characters) usually operates as a "digital key" to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software or digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

17. Visual depictions in the computer environment are usually in the form of "computer graphic files." Computer graphic files are files where photographs have been digitized into computer binary format. Once in this format the graphic file can be viewed, copied, stored, transmitted, and/or printed. Computer graphic files are differentiated by the type of format convention by which they were created. Common types of computer graphic image files encountered are those in a Joint Photographic Experts Group or JPEG format having the ".jpg" file extension, those graphic files in a Graphic Interchange Format or GIF having the ".gif" file extension, and those graphic files in a Tagged Image File format or TIF having the ".tif" file extension. Common video files encountered are those in a Moving Picture Experts Group or MPEG format having the ".mpeg" or ".mpg" file extension and the Audio Video Interleave or AVI format having the ".avi" file extension. Although other file formats exist, these are the most common formats encountered.

18. In your Affiant's experience and after consultations with other agents and experts in the field of child exploitation who have been involved in investigations related to child pornography, it is of great value during a search to secure all photographs of children, regardless of whether or not the photographs meet the definitions of child pornography, in that the photographs are crucial in identifying any victims of child pornography whose images may be contained in law enforcement repositories of victims of child pornography.

CHILD PORNOGRAPHY COLLECTION

19. Based upon your Affiant's training and experience, and after consulting with other investigators working these matters, your Affiant has learned that child pornography distributors/collectors:

19.1 Receive sexual gratification, stimulation, and satisfaction from actual physical contact with children and/or from fantasies they may have while viewing children engaged in sexual activity or in sexually suggestive poses (in person, in photographs, or other visual media) or from literature describing such activity.

19.2 Collect sexually explicit or suggestive materials (hard-core and soft-core pornography) in a variety of media, such as photographs, magazines, motion pictures, video tapes, books, slides and/or drawings or other visual media that they use for their own sexual arousal and gratification. Further, they may use this type of sexually explicit material to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, and to demonstrate the desired sexual acts.

19.3 Almost always possess and maintain their material (pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, security of pornography, "child erotica," etc.) in the privacy of their homes or some other secure location. Child distributors/collectors typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

19.4 Often correspond and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, including email addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

19.5 Distributors/collectors who collect sexually oriented pictures of minors generally prefer not to be without their child pornography and/or child erotica for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

19.6 Child pornography collectors maintain their collections in a safe, secure environment such as a home computer and surrounding area, because this material is illegal, can be difficult to obtain, and can be difficult to replace. These collections are maintained for extended periods of time, if not indefinitely, and are kept close by, usually at their residence to enable the collector to view his collection which he values highly.

19.7 The visual images obtained, traded, and/or sold are prized by child pornography collectors, and have emotional value to the collector. The visual images are intrinsically valuable for trading or selling and therefore are destroyed or deleted only rarely by the collector. These images are often maintained by the offender to blackmail the victim in the future, if necessary.

20. Kenneth V. Lanning is a retired FBI agent and a widely acknowledged expert in the field of child sexual exploitation. Lanning spent 30 years with the FBI's Behavioral Science Unit in Quantico, VA, and in 1997 he received the FBI Director's Award for Special Achievement for his career accomplishments in connection with missing and exploited children. Lanning has aptly noted that many collectors of child pornography "swap pornographic images the way children swap baseball cards" and that "preferential sex offenders with a sexual preference for children...tend to collect predominately child pornography or erotica." (Ibid.) They typically collect things such as "books, magazines, articles, newspapers, photographs, negatives, slides,

movies, albums, digital images, drawings, audiotapes, video recordings and equipment, personal letters, diaries, clothing, sexual aids, souvenirs, toys, games, lists, paintings, ledgers, and photographic and computer equipment all relating to their preferences and interests in a sexual, scientific, or social way.” (Ibid.) It is also common for pedophiles to record their contacts and sexual abuse of children. These collections and records are so important to pedophiles that they tend to keep them for extended periods of time, often years. Lanning has found, moreover, that no matter how much child pornography the collector has, he never seems to have enough, and he rarely throws anything away. Another typical feature of a child pornography collection, according to Lanning, is its constancy. Even if evidence of the existence of child pornography is several years old, Lanning states “chances are [the preferential sex offender] still has the collection now – only it is larger.” (Ibid.) In addition, your Affiant’s experience and training has shown that such material is normally and generally kept in the individual’s office, residence, automobile, or other secure location to ensure convenient and ready access.¹

DETAILS OF THE INVESTIGATION

21. On May 25, 2021, members of the Rio Grande Valley Child Exploitation Investigations Task Force (RGV CEITF) initiated an investigation in an attempt to identify a subject(s), uploading child exploitation material to a Dropbox account. The National Center for Missing and Exploited Children (NCMEC) generated an investigative referral (NCMEC report #86440086) and notified members of the RGV CEITF. The referral was based on information received from Dropbox Inc. regarding a Dropbox account registered to and associated with email address danielmolstad380@gmail.com that is being used to upload child exploitation material.

22. Members of the RGV CEITF reviewed each video/image file of the child exploitative material uploaded into the Dropbox account. Three video files were selected to view as a representative sample to determine that the files did in fact contain child pornography. The following is a description of the video/image files uploaded to the Dropbox account:

23. The first file, " **Video_20171016011137711_by_vidcompact**" is a video file approximately two (2) minutes in length. The video depicts a male infant, approximately 6 to 8 months of age, wearing a white diaper laying on a bed with pillows covering his face. Also, in the frame is an unidentified adult male. The video begins with the adult male removing the infant’s diaper exposing the infant’s genitals. The adult male then masturbates the infant’s penis. Approximately thirty (30) seconds into the video, the frame shifts, and now the infant is on his stomach with his anus and testicles exposed. The adult male puts a lubricant /gel on the infant’s anus and then the adult male digitally penetrates the infant’s anus. Approximately fifty (50) seconds into the video, the adult male reapplies lubricant/gel to the infant’s anus and then inserts his erect penis into the infant’s anus. The adult male continues to anally penetrate the infant for the remainder of the video.

¹ Child Molesters: A Behavioral Analysis, by Kenneth V. Lanning
Fifth Edition, Pub. 2010, by the National Center for Missing & Exploited Children

24. The second file, "6yo_s01" is a video file approximately fifty-nine (59) seconds in length. The video depicts a prepubescent male child, approximately 5 to 6 years of age, standing in a hallway wearing a gray polo shirt. Also, in the video is an unidentified adult male with an erect penis. The video begins with the adult male inserting his erect penis into the child's mouth, which then leads to oral sex. Approximately fifty-five (55) seconds into the video, the adult male ejaculates semen into the child's mouth and the video ends shortly thereafter.

25. The third file, "Video_20171016025940954_by_vodcompact" is a video file approximately one (1) minute and forty (40) second in length. The video depicts a naked prepubescent male child approximately 10-12 years of age, kneeling on the ground. The boy is completely naked except for a red and blue mask. Also, in the video is a naked unidentified male with an erect penis. The video begins with the adult male inserting his erect penis into the child's mouth, which then leads to oral sex. Approximately one (1) minute and (27) seconds into the video, the adult male masturbates over the child's face until he ejaculates onto the child's mouth and face.

Dropbox Inc. BACKGROUND

26. Based on my training and experience, I have learned that web-hosting companies, such as Dropbox, Inc. maintain server computers connected to the Internet. Their customers use those server computers to operate websites on the Internet.

27. In general, web-hosting companies like Dropbox, Inc., ask each of their customers to provide certain personal identifying information when registering for an account. This information can include the customer's full name, physical address, telephone number and other identifiers, email addresses, and business information. Web-hosting companies also may retain records of the length of service (including start date) and types of services utilized. In addition, for paying customers, web hosting companies typically retain information about the customer's means and source of payment for services (including any credit card or bank account number).

28. Web-hosting companies' customers place files, software code, databases, and other data on the servers. To do this, customers connect from their own computers to the server computers across the Internet. This connection can occur in several ways. In some situations, it is possible for a customer to upload files using a special website interface offered by the web-hosting company. It is frequently also possible for the customer to directly access the server computer through the Secure Shell ("SSH") or telnet protocols. These protocols allow remote users to type commands to the web server. The SSH protocol can also be used to copy files to the server. Customers can also upload files through a different protocol, known as File Transfer Protocol ("FTP"). Servers often maintain logs of SSH, Telnet, and FTP connections, showing the dates and times of the connections, the method of connecting, and the Internet Protocol addresses ("IP addresses") of the remote users' computers. Servers also commonly log the port number associated with the connection. Port numbers assist computers in determining how to interpret incoming and outgoing data. For example, SSH, Telnet, and FTP are generally assigned to different ports.

29. Based on my training and experience, and the training and experience of other law enforcement with whom I have spoken, Dropbox, Inc. was founded in 2007 and is a privately held electronic file storage service provider headquartered in San Francisco, California. Dropbox, Inc. uses cloud computing to enable users to store and share files and folders with other users across the Internet using file synchronization. Dropbox, Inc. provides both free and fee-based file sharing and file synchronization services. Dropbox, Inc. conducts business throughout the United States and the world through its cloud-computing based file sharing services.

30. Dropbox, Inc. offers a client application to facilitate the file synchronization and access on a wide variety of operating systems and devices owned or used by the account holder. Dropbox, Inc. allows a user to create a Dropbox, Inc. account which is identified by the user's email address and it is secured with a user password. The email address is the unique identifier for a Dropbox, Inc. account. Once an account is created with Dropbox, Inc., the user must enter his or her email address for the account along with a valid user-created password in the login screen in order to access the account. Since Dropbox, Inc. accounts are not publicized and the general login screen does not show other valid email accounts, the user must know the email address in the first step to access a Dropbox, Inc. account.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

31. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Dropbox, Inc. to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment "B". Upon receipt of the information described in Section I of Attachment "B", government authorized persons will review that information to locate the items described in Section II of Attachment "B".

APPLICATION

32. Based on the aforementioned factual information, your Affiant respectfully submits that there is probable cause to believe that the Dropbox account registered to the email address danielmolstad380@gmail.com contains evidence of distribution, receipt, and possession of child pornography in violation of 18 U.S.C. 2252 and 2252A. And that the following property, evidence, fruits and instrumentalities of these offenses are located within the Dropbox, Inc. account danielmolstad380@gmail.com and stored on computers maintained by Dropbox, Inc.

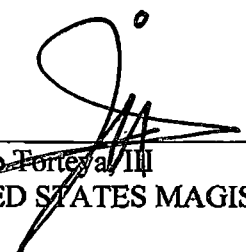
33. This Court has jurisdiction to issue the requested warrant because it is a "court of competent jurisdiction," as defined by 18 U.S.C. ' 2711, 18 U.S.C. ' 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A). Specifically, the Court is "a district court of the United States...that - has jurisdiction over the offense being investigated."

34. Your Affiant, therefore, respectfully requests that the attached warrant be issued authorizing the search of the Dropbox, Inc. account registered to the email address danielmolstad380@gmail.com that is stored at the premises owned, maintained, controlled, and/or operated by Dropbox, Inc., a company headquartered at Dropbox, Inc., 1800 Owens St. Ste. 200. San Francisco, CA 94158 and authorizing the search and seizure of the items described in Attachment B.



Ian Kelly
Special Agent
Homeland Security Investigations

Submitted by reliable electronic means,
sworn to and signature attested as per
Fed. Rules Cr. Proc. 4.1, this
28th day of January, 2022.



Ignacio Portey
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT "A"
PROPERTY TO BE SEARCHED

This warrant applies to information associated with the DropBox.com account registered to the email address danielmolstad380@gmail.com, (User ID 3715727344) which is stored at premises owned, maintained, controlled, or operated by Dropbox.com, 1800 Owens St. Ste. 200 San Francisco, CA 94158.

ATTACHMENT "B"
PARTICULAR THINGS TO BE SEIZED

I. Information to be disclosed by Dropbox.com

To the extent that the information described in Attachment C is within the possession, custody, or control of Dropbox.com including any emails, records, files, logs, or information that have been deleted but are still available to Dropbox.com, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Dropbox.com is required to disclose the following information to the government for each account or identifier listed in Attachment C:

- a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- b. The types of service utilized;
- c. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, videos and files;
- d. All records pertaining to communications between Dropbox.com, and any person regarding the account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and

instrumentalities of violations of 18 U.S.C. §§ 2252 and 2252A, involving danielmolstad380@gmail.com including, for each account or identifier listed on Attachment C, information pertaining to the following matters:

- a. All images depicting children engaging in sexually explicit conduct as defined in 18 U.S.C. § 2256
- b. All electronic communications regarding children engaging in sexually explicit conduct;
- c. All communications with potential minors involving sexual topics or in an effort to seduce the minor.
- d. Any evidence that would tend to identify the person using the account when any of the items listed in subparagraphs a-c were sent, read, copied or downloaded.
- e. Records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts.